APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/586,907	06/05/2000	Rajesh G. Shakkarwar	0100.0000370	9317

24228   7590   05/13/2004

MARKISON & RECKAMP, PC
PO BOX 06229
WACKER DR
CHICAGO, IL 60606-0229

EXAMINER
VAUGHAN, MICHAEL R

ART UNIT	PAPER NUMBER
2131	5

DATE MAILED: 05/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/586,907	SHAKKARWAR, RAJESH G.
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>24 March 2004</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-69* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-69* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

Detailed Office Action

Claims 1-69 have been fully reconsidered and are pending.

Response to Arguments

1. Applicant's arguments filed 3-24-04 have been fully considered but they are not persuasive.

Applicant argues on page 3 of the immediate response that the Office Action fails to establish where Fisherman recites, "receiving in a protection engine, an interface control command." Examiner respectfully disagrees. Examiner supplied citations from the Fisherman reference as a guide to where the examiner felt Fisherman anticipated the limitations of the claims. The examiner however does not rely solely on the recited passages from Fisherman. Applicant is encouraged to consider the teachings throughout the Fisherman patent and not just the references indicated by the examiner. With that in mind, Fisherman clearly teaches receiving a control command handler, which obviously receives control commands to handle (column 4, lines 2-3).

Examiner notes that many of the Applicant's arguments are based on subtle differences of the words used in the Fisherman patent and those in the claimed invention. According to the MPEP 2106,

Office personnel are to give claims their broadest reasonable interpretation in light of the supporting disclosure. In re Morris, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim are not read into the claim. In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA 1969). See also In re Zletz, 893 F.2d 319, 321-22, 13 USPQ2d 1320, 1322 (Fed. Cir. 1989) ("During patent examination the pending claims must be interpreted as broadly as their terms reasonably allow.... The reason is simply that during patent prosecution when claims can be amended, ambiguities should be recognized, scope and breadth of language explored, and clarification imposed.... An essential purpose of patent examination is to fashion claims that are precise, clear, correct, and unambiguous. Only in this way can uncertainties of claim scope be removed, as much as possible, during the administrative process.").

Furthermore when pointing out the differences in the Fisherman patent with those in the claimed invention, Applicants bases his arguments on a very narrow interpretation of the language. Examiner has given the words in both the Fisherman reference and the claimed invention their broadest reasonable interpretation. Particular instances will be discussed in this Office Action henceforth.

Applicant argues on page 4 of the immediate response that Fisherman fails to disclose "a security risk" let alone determine whether the interface control command introduces a security risk. Examiner respectfully disagrees. Security risks as taught by are commands that can cause potential damage to the system. These commands must only be executed from authorized program entities. Examiner relies on the specification of Fisherman in columns 5-7 for support of this interpretation. The system must be able to recognize individual commands if it is able to differentiate between potentially threatening commands and lesser important commands.

Applicant argues on page 5 of the immediate response that Fisherman patent does not teaches determining a state of a switch. Examiner interprets a switch as a change between at least two states. Switches can be implemented in hardware or software. It is a fine line between hardware and software switches for the reason that eventually all software must be implemented at the hardware level. Certainly, a switch is not just a transistor. With that in mind, Fisherman's system has two states, an active state (protected) and a passive state (unprotected). Fisherman teaches that PPSM determines the state of the machine by interpreting which flags are set. The state of the flags effectively constitutes a switch because when the flags are changed the system changes from an active state to a passive state, see column 4, lines 26-32. The system does this when a program issues a command, which may or may not pose a security risk. As stated previously, the system is fully capable of determining which commands pose security risks.

Applicant argues on page 6 of the immediate response that Fisherman fails to describe an interface control command let alone "inhibiting execution of the interface control command. As stated above, Fisherman teaches an interface control command in column 4, lines 2-3. Fisherman also states that when the system is in the active state the commands are hidden and therefore cannot be executed by the CPU. This is synonymous to inhibiting the interface control command.

Applicant poses similar arguments for the other independent claims 33, 64, and

67, to which the examiner supplies the same aforementioned response.

On page 9 of the immediate response, Applicant argues that Fisherman fails to

describe a protection engine. Fisherman teaches many modules to his system

including a set of protection programs, disk-request handler, a control-command

handler, a protection control program, set of key programs, which include the initial key

program, the command-handler key program, and the request-handler key program

(column 4, lines 1-6) and even a programmable controller (column 4, line 40). Which of

these modules equates to the claimed "protection engine" is really a moot point based

on how one interprets a "protection engine". What really matters is that the elements of

Fisherman's system function in such a way that anticipates the claimed invention.

On page 10, Applicant argues that Fisherman fails to teach, "determining when

the execution of the interface control command has been completed". Examiner

respectfully disagrees. In column 14, lines 31-36, Fisherman clearly teaches the

interface control command is able to determine when the received command is finished

because once that is done, the system is switched back to an active state.

With regards to the Applicant's allegation that Fisherman does not disclose an

electrical switch on page 10, examiner cites the previous interpretation of a switch.

Applicant alleges that Fisherman fails to teach the use of any cryptographic techniques on page 11. Examiner respectfully disagrees. In column 9, lines 26-28, Fisherman discloses a relationship between a signature and a flag, which controls the state of the system. Fisherman discloses that the software have signatures that must be verified. Signatures are well known in the art of cryptography as a means to provide authorization that is very hard to reproduce, similar to handwritten signatures. Of course signatures in computers are even more difficult to produce and therefore are a way to prove authorization.

Applicant alleges that Fisherman fails to teach a hard disk drive formatting command on page 12 of the immediate response. While Fisherman does not come out and explicitly state that a format command is a high security risk, he does say that commands altering the boot sector of a hard disk are monitored. Thus, Fisherman suggests that those commands, which alter the underlying structure of a hard disk, are not to be carelessly executed. A hard disk formatting command is clearly this type of command and one of ordinary skill in the art would make this connection from Fisherman's suggestion in column 6, lines 64-66.

Applicant alleges that Fisherman fails to teach issuing a challenge to the source of the interface control command on page 12 of the immediate response. Examiner respectfully disagrees. In column 14, lines 10-23, Fisherman addresses the notion of programs having to provide the necessary authorization in order to execute a command.

This shows an underlying notion of the program responding to a challenge. Moreover,

the program must always be able to show it is authorized. Fisherman may not explicitly

state that the system sends a challenge each time but each time the program wants to

execute a command it must give authorization. Applicant is interpreting the invention

very narrowly. A broad and reasonable interpretation of this teaching clearly suggests

that the system is effectively requiring a positive response from a program before

allowing execution of a command.

Applicant alleges that Fisherman does not disclose comparing the response to a

mathematical function of a value accessible only to the protection engine and to an

operating system on page 13. Examiner cites the Fisherman's description of signatures

in column 1, lines 63-66 and use of a protection memory. Fisherman uses signature in

his invention as well. Signatures, as stated above are well know in the art as a form of

identification. Signatures are constructed by a mathematical formula. In column 14,

lines 18-20, the signatures are compared with that of a record in a controlled memory.

Applicant alleges that Fisherman does not disclose writing a value from the

processor to a one-time writable register on page 14. Fisherman discloses that a

protected memory subsystem (which are registers) are used one time only prior to

loading the initial software (column 1, lines 40-45).

Applicant alleges that Fisherman does not disclose a timer on page 14.
Examiner is interpreting the references on column 11, lines 37-50 as a means to setting
a time limit to the session. Fisherman's system clearly has a way to end a session so
that the active (protected) can be restored. The suggestion is that the system is more
susceptible to security risks when it is in the passive mode. Therefore, there must be a
way to prevent the system from remaining in that mode. Fisherman teaches a time at
which the system is switch back so one can interpret this feature as time expiration.
Therefore, one of ordinary skill in the art would make the connection a watchdog timer
for example.

Applicant alleges that Fisherman does not teach an interface control command
execution completion sensor. Examiner cites the reference in column 14, lines 30-35
where Fisherman clearly teaches this feature. Again applicant is portraying a very
narrow interpretation of the words in both the claim invention and the patented
invention.

In response to the allegation that there is no motivation to combine the teachings
of GITAT and Fisherman, the examiner assumes the Applicant misconstrued the
intention of the combination. The GITAT reference was merely cited to give the
generally accepted definition of the terms such as parallel port, serial port, USB port,
and IEEE-1394 port. Examiner did not intend to show one of ordinary skill in the art
would be motivated to combine a computer dictionary with the teachings of Fisherman.

Rather, the examiner intended to show that because Fisherman taught an invention

which resides in a computer having a bus that these ports which operate on buses

within a computer would be an obvious addition one of ordinary skill in the would make.

One of ordinary skill in the art would have been motivated merely by the knowledge of

data following on computer buses within a computer system that the protection offered

by Fisherman's system could be expanded to these types of areas.

In response to applicant's argument that computer protection and a management

controller is nonanalogous art, it has been held that a prior art reference must either be

in the field of applicant's endeavor or, if not, then be reasonably pertinent to the

particular problem with which the applicant was concerned, in order to be relied upon as

a basis for rejection of the claimed invention. See In re Oetiker, 977 F.2d 1443, 24

USPQ2d 1443 (Fed. Cir. 1992). In this case, Davis's invention is a computer system

management apparatus and Fisherman's invention relates to the management of

computer data within a computer system. There is no question of nonanalogous

between to the two inventions. Both inventions share the common goal of protecting

computers systems with a management system.

Claim Rejections - 35 USC ' 102

2. Claims 1-12, 19-21, 24, 27, 33-39, 45-47, 50, 53, 59-61, 64-69, are rejected

under 35 U.S.C. 102(b) as being anticipated by Fisherman et al (USP 5,586,301).

As per claim 1, Fisherman et al teach a method for protection of computer assets

from unauthorized access comprising the steps of:

receiving in a protection engine, an interface control command (column 3,

lines 33-36);

determining whether the interface control command introduces a security

risk (column 4, lines 23-30 and column 5, lines 7-11);

when the interface control command introduces a security risk,

determining a state of a switch (column 4, lines 20-33);

when the state of the switch is a protected state, inhibiting execution of the

interface control command (column 4, lines 38-42); and

when the state of the switch is an unprotected state, allowing execution of

the interface control command (column 4, 20-24).

As per claim 33, Fisherman et al teach a method for protection of computer

assets from unauthorized access comprising the steps of:

receiving in a protection engine, an interface control command (column 3,

lines 33-36);

determining whether the interface control command introduces a security

risk (column 4, lines 23-30 and column 5, lines 7-11);

when the interface control command introduces a security risk,

determining whether of a source of the interface control command is authentic

(column 14, 16-19);

when the source of the interface control command is not authentic,

inhibiting execution of the interface control command (column 14, lines19-24);

and

when the source of the interface control command is authentic, allowing

execution of the interface control command (column 14, lines 25-28).

As per claims 2 and 34, Fisherman et al teach the step of inhibiting execution of

the interface control command further includes the step of:

providing an indication that the execution of the interface control command

was inhibited (column 6, line 65).

As per claim 3, Fisherman et al teach changing the state of the switch to the

protected state when a timeout duration has elapsed (column 11, lines 50-53).

As per claim 4, Fisherman et al teach determining when the execution of the

interface control command has been completed; and

when the execution of the interface control command has been

completed, changing the state of the switch to the protected state (column 14, lines 30-

35).

As per claim 5, Fisherman et al teach determining the state of an electrical switch

(column 4, lines 29-30).

As per claim 6, Fisherman et al teach determining the state of a software-based

switch (column 4, lines 29-30 and 38-42).

As per claim 7, Fisherman et al teach using cryptographic techniques to

determine the state of the software-based switch (column 4, lines 25-30).

As per claims 8 and 35, Fisherman et al teach allowing data to be written to a

hard disk drive (column 4, lines 23-24).

As per claims 9 and 36, Fisherman et al teach allowing data to be written to a.

boot sector of the hard disk drive (column 5, lines 11-15).

As per claims 10 and 37, Fisherman et al teach allowing data to be written to a

file allocation table of the hard disk drive (column 5, lines 16-22).

As per claims 11 and 38, Fisherman et al teach allowing data to be written to a floppy disk drive (column 11, lines 65-67).

As per claims 12, 27, 39, and 53, Fisherman et al teach allowing data to be written to a BIOS memory (column 3, lines 55-63).

As per claims 19 and 45, Fisherman et al teach determining whether the interface control command is a hard disk drive formatting command. Fisherman et al teach that the system is able to detect write operations to the hard drive (column 5, lines 7-10). Specifically the system can detect write commands to the entire cluster (column 5, lines 30-35). Also Fisherman et al teach that proposed changes are analyzed in order to prevent unsanctioned changes in the protected files and directories. Therefore, it is inherent that Fisherman et al teach determining whether the interface control command is a hard disk drive formatting command because a format function erases all data from the hard drive partition.

As per claims 20 and 46, Fisherman et al teach determining whether the interface control command is a boot sector write command (column 6, lines 64-66).

As per claims 21 and 47, Fisherman et al teach determining whether the interface control command is a program file write command (column 5, lines 26-30).

As per claims 24 and 50, Fisherman et al teach determining whether the interface control command changes a file attribute, the file attribute enabling or disabling execution of a file corresponding to the file attribute (column 13, lines 55-65).

As per claim 59, Fisherman et al teach the step of determining whether the source of the interface control command is authentic comprises the step of:

issuing a challenge to the source of the interface control command (column 14, lines 10-15);

receiving a response from the source of the interface control command (column 14, lines 16-18); and

determining whether the response is valid (column 19-22).

As per claim 60, Fisherman et al teach the step of determining whether the response is valid comprises the step of:

comparing the response to a mathematical function of a value accessible only to the protection engine and to an operating system (column 1, lines 63-66).

As per claim 61, Fisherman et al teach writing the value from a processor to a one-time-writable register in the protection engine (by an operating system) during a boot process (before application software is enabled) (column 1, lines 45-55).

As per claim 64, Fisherman et al teach an apparatus for protection of computer

assets from unauthorized access comprising:

an interface controller operatively coupled to receive a interface control

command to control an interface device (column 3, lines 33-36);

a switch selectable between a protected state and an unprotected state

(column 4, lines 20-33);

a protection engine operatively coupled to the interface controller to

receive the interface control command (see Fig. 1) and operatively coupled to the switch

to detect whether the electrical switch is in the protected state or the unprotected state

(column 4, lines 29-30) to determine whether the interface control command poses a

security risk (column 4, lines 23-30 and column 5, lines 7-11) and to selectively inhibit

or allow execution of the interface control command by the interface controller

depending on whether or not the interface control command poses the security risk and

depending on whether the switch is in the protected state or the unprotected state

(column 14, lines19-28).

As per claim 65, Fisherman et al teach a timer operatively coupled to the switch

to reset the switch to the protected state after a period of time has elapsed (column 11,

lines 50-53).

As per claim 66, Fisherman et al teach the switch to reset the switch to the

protected state after an execution of the interface control command has been completed

(column 14, lines 30-35).

As per claim 67, Fisherman et al teach an apparatus for protection of computer assets from unauthorized access comprising:

an interface controller operatively coupled to receive a interface control command to control an interface device (column 3, lines 33-36);

a protection engine operatively coupled to the interface controller for preventing unauthorized access to the interface device and operatively coupled to receive the interface control command to determine whether a source of the interface control command is authentic and to selectively allow or inhibit execution of the interface control 5 command by the interface controller depending on whether or not the source of the interface control command is authentic (column 14, lines 19-34).

As per claim 68, Fisherman et al teach a one-time-writable register operatively coupled to the protection engine to store a value used to determine whether the source of the interface control command is authentic (column 1, lines 45-55).

As per claim 69, Fisherman et al teach the value is accessible only to the protection engine and to an operating system (column 1, lines 51-54).

Claim Rejections - 35 USC ' 103

3. Claims 13-17, 28-32, 40-44, 54-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fisherman et al in view of Glossary of Information Technology Acronyms and Terms (here within GITAT).

As per claims 13-16, 28-32, 40-44, and 54-58, Fisherman et al teachings controlling write access to the hard drive (column 4, lines 20-25). Fisherman et al is silent in disclosing allowing data to be written to a parallel port, serial port, USB port, and a IEEE-1394 port. Fisherman et al does teach a computer system which controls data access to the system's basic input output system (see abstract). GITAT teaches that a parallel port, serial port, USB port, and an IEEE-1394 port are examples of computer input output ports (pgs. 138, 248, 295, and 337). One of ordinary skill in the art would know how to control the I/O ports of a computer system. It would be advantageous to the system's security to only allow authorized entities to have access to write data to these ports. An unauthorized person might try to send sensitive data via an output port whereas an authorized person may need to use the output port in a legitimate. Clearly, the system's security would be highly stronger if the system could control access to the I/O ports.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of GITAT within the system of Fisherman et al because it would allow the system to grant or deny data written to I/O

port, thereby greatly improving the system's ability to monitor and control data.

As per claim 17, Fisherman et al teachings controlling write access to the hard drive (column 4, lines 20-25). Fisherman et al is silent in disclosing allowing data to be written to a flash memory device. GITAT teaches that a flash memory device is a nonvolatile storage chip. Hard drives are also nonvolatile. Therefore, Fisherman et al teach controlling data written to nonvolatile memory. Fisherman et al disclose a secure system whereby the security comes from monitoring and controlling access to memory.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of GITAT within the system of Fisherman et al because it would allow the system to control data written to flash memory devices, thereby greatly improving the system's ability to monitor and control data.

4. Claims 18, 25, 26, 51, 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fisherman et al and GITAT as applied to claims 1 and 13 above, and further in view of Davis (USP 6,205,547).

As per claims 18, 25, 26, 51, and 52, Fisherman et al teach a system controller which intercepts commands to control the hard drive controller (see abstract).

Fisherman et al fail to teach controlling commands sent to the thermal management

controller. Davis teaches a thermal management controller which closely monitors and

alters a computer's systems thermal conditions separately from the operating system

(column 6, lines 9-16). Davis teaches that CPU fans are controlled by the thermal

controller to regulate CPU temperature (column 5, lines 40-45). Fisherman's system

also works independent of the operating system so it too cannot be influenced by

processes of the operating system. Davis's thermal management controller provides

the necessary control to keep the computer system functioning properly. Therefore, it

would be highly advantageous to control which entity can write data to the thermal

controller. Clearly, commands that try to turn off CPU fans, would not be allowed be

allowed by unauthorized entities.

In view of this, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to employ the teaching of Davis within the system of

Fisherman et al and GITAT because it would permit regulation of the thermal dynamics

of the system by providing a secure method of communication with the thermal

management controller.

5. Claims 22, 23, 48, 49 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Fisherman et al in view of Chen et al (USP 5,832,208).

As per claims 22, 23, 48, 49, Fisherman et al teaches a system which analyzes

commands which change the content of hard disks. Fisherman et al is silent in

expressing disclosing determining whether the file extension is an executable file extension including file extensions of an exe extension, a com extension, a bat extension, or a bin extension. Chen et al discloses a system with detects and removes computer viruses (see abstract). Specifically, Chen et al discloses that computer viruses are attached to executable files with an exe extension, a com extension, a bat extension, or a bin extension so that they may infect a system (column 2, lines 8-10).

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Chen et al within the system of Fisherman et al because it would allow the system to recognize additional types of commands that could potentially harm the computer system.

6. Claims 62 and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fisherman et al in view of Applied Cryptography 2nd Edition (here within AC).

As per claim 62 and 63, Fisherman et al teach the step of determining whether the response is valid comprises the step of comparing the response to the correct response value. Fisherman et al are silent in expressly disclosing performing a mathematical operation on the challenge to produce a correct response value. AC teaches performing a mathematical operation on the challenge to produce a correct response value (pg. 53). AC uses pseudorandom numbers to form the challenge value. A mathematical operation is performed on each challenge so that each authentication attempt is unique and cannot be replayed.

In view of this, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to employ the teaching of AP within the system of

Fisherman et al because it would allow the system to authenticate commands in which

each authentication attempt is unique and highly secure.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Michael R Vaughan whose telephone number is 703-

305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for

the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Michael R Vaughan
Examiner
Art Unit 2131

MV

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100